

E-Mail-Verschlüsselung

Schritt 1: Software installieren

- **GnuPG** zur Verschlüsselung der E-Mails.
 - Linux: meistens schon installiert
 - Windows: GPG4Win <https://www.gpg4win.org/> (Minimale Installation oder Vanilla-Version reichen)
 - Mac: GPGTools <https://gpgtools.org/>
- E-Mail-Programm **Thunderbird** zur Verwaltung der E-Mails.
 - <https://www.mozilla.org/de/thunderbird>
 - Beim ersten Aufruf E-Mail-Konto konfigurieren und Feineinstellung durchführen (S. 4)
- Thunderbird-Add-On **Enigmail**, die Schnittstelle zu GnuPG.
 - In Thunderbird unter **Extras** → **Add-Ons** nach Enigmail suchen und installieren.

Schritt 2: Schlüssel erstellen

Mit dem Assistenten:

- Wähle in der Menüleiste von Thunderbird: **Enigmail** → **Einrichtungs-Assistent**.
 - Tipp: Lies die Texte des Assistenten in Ruhe durch.
- Wähle die **ausführliche Konfiguration** für Fortgeschrittene.
- Wähle das E-Mail-Konto, für das die Schlüssel gelten sollen.
- Gib eine **Passphrase** ein.
 - Diese musst du immer eingeben, wenn du auf den Schlüssel zugreifen willst, um Missbrauch des Schlüssels zu verhindern. Du kannst sie später ändern.
- Schlüssel wird erzeugt, dies kann eine Weile dauern.
- Erzeuge das **Widerrufszertifikat**.
 - Damit kannst du deinen öffentlichen Schlüssel von Key-Servern widerrufen, auch nach Verlust des privaten Schlüssels (oder der Passphrase).

Oder manuell:

- Wähle in der Menüleiste von Thunderbird: **Enigmail** → **Schlüssel verwalten**
- Dann **Erzeugen** → **Neues Schlüsselpaar**
- Wähle das E-Mail-Konto, für das die Schlüssel gelten sollen
- Gib eine **Passphrase** ein
- Ablaufdatum nicht länger als 5 Jahre
- Unter Erweitert: Schlüsselstärke **4096** Bit, Algorithmus RSA
- Schlüssel erzeugen, dies kann eine Weile dauern
- Erzeuge das **Widerrufszertifikat**

Schritt 3: öffentliche Schlüssel importieren/exportieren

Zur Verschlüsselung verwendet man den **öffentlichen Schlüssel der Empfängerin**. Also: damit andere Personen dir verschlüsselte E-Mails schicken können, brauchen sie deinen öffentlichen PGP-Schlüssel.

Den öffentlichen Schlüssel auf Key-Server hochladen:

Key-Server sind die bequemste Möglichkeit. Dort kann dein Schlüssel einfach gefunden werden, allerdings sind die im Schlüssel eingetragenen E-Mail-Adressen dann öffentlich.

- Wähle in der Menüleiste von Thunderbird: **Enigmail** → **Schlüssel verwalten**
- Setze einen Haken bei **Standardmäßig alle Schlüssel anzeigen**
- **Rechtsklick** auf deinen Schlüssel, auf Schlüsselserver hochladen

Oder den öffentlichen Schlüssel direkt an Kommunikationspartner schicken:

- Wähle in der Menüleiste von Thunderbird: **Enigmail** → **Schlüssel verwalten**
- **Rechtsklick** auf deinen Schlüssel, **Öffentliche Schlüssel per E-Mail senden**

Um anderen Personen verschlüsselte Nachrichten schreiben zu können, brauchst du wiederum deren öffentlichen PGP-Schlüssel.

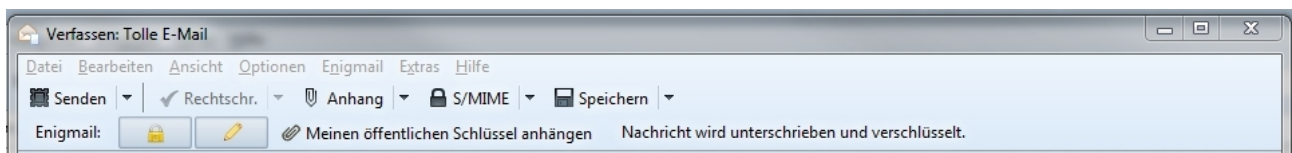
Auf Key-Server suchen:

- Wähle in der Menüleiste von Thunderbird: **Enigmail** → **Schlüssel verwalten**
- Dann **Schlüsselserver** → **Schlüssel suchen**, um einzelne Schlüssel zu finden
- Oder **Schlüsselserver** → **Schlüssel für alle Kontakte suchen** (damit gibst du allerdings dem Key-Server dein Kontakt-Netzwerk bekannt)

Oder Schlüssel aus E-Mail-Anhang importieren:

- Der PGP-Schlüssel hat die Dateierendung .asc
- Rechtsklick auf die Datei: PGP-Schlüssel importieren.

Schritt 4: E-Mails unterschreiben und verschlüsseln



- Neue E-Mail in Thunderbird verfassen
- Stelle sicher, dass **unterschreiben** und **verschlüsseln** aktiviert ist
 - Verschlüsseln setzt voraus, dass der Empfänger auch PGP nutzt
 - Unterschreiben geht immer – auch wenn Empfänger nichts damit anfangen können
- Zum Unterschreiben muss du beim Senden deine **Passphrase** eingeben

Bonusmaterial I: Schlüssel unterschreiben (Key-Signing)

Du kannst öffentliche PGP-Schlüssel von anderen Leuten unterschreiben. Damit bestätigst du die Zuordnung des Schlüssel zu dieser Person. So entsteht ein „Vertrauensnetzwerk“ (Web of Trust): Wer die andere Person nicht kennt, aber dich kennt und dir vertraut, kann auch dem Schlüssel der anderen Person vertrauen. Allerdings wird dadurch möglicherweise dein Kontakt-Netzwerk auf einem Key-Server öffentlich einsehbar. Überlege dir also, wessen Keys du signierst.

Überprüfe, ob der besagte Schlüssel zu der Person gehört:

- Wenn ihr Name in der E-Mail-Adresse vorkommt: prüfe z.B. per Personalausweis
- Sonst: lasse dir von ihr eine verschlüsselte und unterschriebene E-Mail schicken mit einem Inhalt, den du dir im direkten Kontakt ausdenkst und mitteilst.

Gleiche den Schlüssel-Fingerabdruck ab:

Als erstes überprüfst du, ob der Schlüssel, den die andere Person besitzt, dem öffentlichen Schlüssel entspricht, den du von ihr hast. Dies geht über den weltweit eindeutigen Fingerabdruck.

- Lasse dir den öffentlichen Schlüssel per Mail schicken oder lade ihn vom Key-Server
- Wähle in der Menüleiste von Thunderbird: **Enigmail** → **Schlüssel verwalten**
- **Rechtsklick** auf den Schlüssel → **Schlüsseleigenschaften**
- Lasse dir von der anderen Person den Fingerabdruck ihres Schlüssel geben
 - ausgedruckt auf Papier
 - oder diktieren etc.

Schlüssel unterschreiben

- Wähle in der Menüleiste von Thunderbird: **Enigmail** → **Schlüssel verwalten**
- **Rechtsklick** auf den Schlüssel → **Unterschreiben**
- Zum Signieren musst du deine **Passphrase** eingeben

Den signierten Schlüssel seinem Besitzer schicken:

- Wähle in der Menüleiste von Thunderbird: **Enigmail** → **Schlüssel verwalten**
- **Rechtsklick** auf den Schlüssel → öffentlicher Schlüssel per E-Mail senden

Wenn jemand anderes deinen Schlüssel signiert hat und dir schickt, kannst du ihn auf einen Keyserver hochladen, wenn du möchtest. Falls dein Schlüssel dort schon liegt, wird er aktualisiert.

Unterschriften einsehen:

- Wähle in der Menüleiste von Thunderbird: **Enigmail** → **Schlüssel verwalten**
- **Rechtsklick** auf den Schlüssel → **Schlüsseleigenschaften** → Reiter **Zertifikate**

Bonusmaterial II: Feineinstellung

- Einstellungen in Thunderbird korrigieren: ≡ **Menübutton** → **Einstellungen** → Icon **Erweitert** → Reiter **Allgemein** → Knopf **Konfiguration bearbeiten ...** und
 - JavaScript deaktivieren: **javascript** ins Suchfeld eingeben, Einstellung **javascript.enabled** finden; falls **true**, per Doppelklick auf **false** setzen
 - Falls gewünscht, dafür sorgen, dass neue Mails oben stehen: **sort_order** ins Suchfeld eingeben, die beiden mit **mailnews** beginnenden Einträge doppelklicken, Wert **2** eingeben, Enter (gilt nur für Mail-Ordner, die noch nicht geöffnet wurden)
- Eine Einstellung nach der Installation von Enigmail, ohne die manche Mails nicht entschlüsselt werden:
 - ≡ **Menübutton** → **Add-Ons** → im Fenster links **Erweiterungen** → bei **Enigmail** den Knopf **Einstellungen** klicken
 - Falls Reiter **Erweitert** nicht vorhanden, im Reiter **Allgemein** den Knopf **Experten-Optionen und -Menüpunkte anzeigen** klicken
 - Reiter **Erweitert** → Haken entfernen bei **Anhänge nur herunterladen, wenn diese geöffnet werden sollen (nur bei IMAP)**
 - falls gewünscht, wieder zurück zum Reiter **Allgemein** und Knopf **Experten-Optionen und -Menüpunkte ausblenden** klicken
 - Einstellungen mit **OK** schließen